CLAIMS

We claim:

1. A method for adjusting an m-bit CRC of a sub-message, wherein the CRC generating polynomial is primitive or irreducible and the sub-message corresponds to a composite sub-message having n trailing zeroes, comprising:

storing the m-bit CRC in an m-bit memory location;

examining each bit of N, where N equals n mod ($2^m - 1$), in order from the most significant bit to the least significant bit; the examining act for each examined bit comprising:

finite field squaring the contents of the m-bit memory location, and;

if the examined bit equals one, advancing the contents of the m-bit memory location to the next state as determined by the Galois field defined by the CRC generating polynomial.

2. The method of claim 1, wherein the CRC generating polynomial is a primitive polynomial.

3. The method of claim 1, wherein the CRC generating polynomial is an irreducible polynomial

4. The method of claim 1, wherein for each examined bit equaling one, the finite field squaring act and the advancing the contents act are performed simultaneously.

5. A method for adjusting an m-bit CRC of a sub-message, wherein the sub-message corresponds to a composite sub-message having n trailing zeroes and the m-bit CRC is equal or congruent to one, comprising:

storing the m-bit CRC in an m-bit memory location;

examining each bit of N, where N equals n mod (2^m-1), in order from the most significant bit to the least significant bit; the examining act for each examined bit comprising:

finite field squaring the contents of the m-bit memory location, and;

if the examined bit equals one, advancing the contents of the m-bit memory location to the next state as determined by the Galois field defined by the CRC generating polynomial.

6. The method of claim 5, wherein the CRC generating polynomial is neither primitive nor irreducible.

7. A method for adjusting an m-bit CRC of a sub-message, the sub-message corresponding to a composite sub-message having n trailing zeroes, wherein the CRC generating polynomial is P(x), comprising:

(a) computing $Y = x^n \bmod P(x)$ using a lookup table;

(b) field multiplying the partial m-bit CRC and Y together; and

(c) field dividing the result from act (b) by P(x), wherein the remainder forms the adjusted partial m-bit CRC.

8. The method of claim 7, wherein act (a) comprises:

(d) factoring x^n into powers of two;

(e) computing the modulus P(x) of each factor from act (d) using a lookup table, and

(f) computing Y by field multiplying together the results from act (e).

9. The method of claim 8, wherein P(x) represents a 32 bit number and the lookup table is no larger than 17 32-bit entries.

10. A method for adjusting an m-bit CRC of a sub-message, the sub-message corresponding to a composite sub-message having n trailing zeroes, wherein the CRC generating polynomial is P(x) and n is less than m, comprising:

(a) computing $Y = x^n \bmod P(x)$ by setting $Y = x^n$;

(b) field multiplying the partial m-bit CRC and Y together by shifting the partial m-bit CRC to the left by n bits; and

(c) field dividing the result from act (b) by P(x), wherein the remainder forms the adjusted partial m-bit CRC.

11. A method of adjusting a CRC of a message composed of a plurality of sub-messages wherein the adjustment is in response to changes in a given sub-message, the given sub-message having a first m-bit CRC and corresponding to a first composite sub-message having n trailing zeroes, the changed sub-message having a second m-bit CRC and corresponding to a second composite sub-message having n trailing zeroes, and wherein the CRC generating polynomial is primitive or irreducible, comprising:

storing the first m-bit CRC in a first m-bit memory location;

examining each bit of N, where N equals n mod $(2^m - 1)$, in order from the most significant bit to the least significant bit; the examining act for each examined

bit comprising:

finite field squaring the contents of the first m-bit memory location, and

if the examined bit equals one, advancing the contents of the first m-bit memory location to the next state as determined by the Galois field defined by the CRC generating polynomial, whereby the first m-bit memory location stores a third CRC of the first composite sub-message;

modulo 2 subtracting the third CRC from the CRC of the message to produce an intermediary CRC;

storing the second m-bit CRC in a first m-bit memory location;

examining each bit of N in order from the most significant bit to the least significant bit; the examining act for each examined bit comprising:

finite field squaring the contents of the second m-bit memory location, and;

if the examined bit equals one, advancing the contents of the second m-bit memory location to the next state as determined by the Galois field defined by the CRC generating polynomial, whereby the second m-bit memory location stores a fourth CRC of the second composite sub-message;

modulo 2 adding the fourth CRC to the intermediary CRC to produce the adjusted CRC of the message.

12. The method of claim 11, wherein the first and second memory locations are the same.

13. The method of claim 11, wherein the CRC generating polynomial is primitive.

14. The method of claim 11, wherein the CRC generating polynomial is irreducible.

15. A method of advancing an m-bit sequence through n states of a Galois field generated by a primitive or irreducible polynomial of degree m, comprising:

storing the m-bit sequence in an m-bit memory location;

examining each bit of N, where N equals n mod $(2^m - 1)$, in order from the most significant bit to the least significant bit; the examining act for each examined bit comprising:

finite field squaring the contents of the m-bit memory location, and; if the examined bit equals one, advancing the contents of the m-bit memory location to the next state as determined by the Galois field.

16. The method of claim 15, wherein the polynomial is a primitive polynomial.

17. The method of claim 15, wherein the polynomial is an irreducible polynomial.